Coronavirus-themed phishing templates used to capture personal information

by **Lance Whitney** in **Security** on May 15, 2020, 8:12 AM PST

Spoofing government and health organizations, these templates help attackers create and customize their own phishing pages to exploit the COVID-19 pandemic, says Proofpoint.

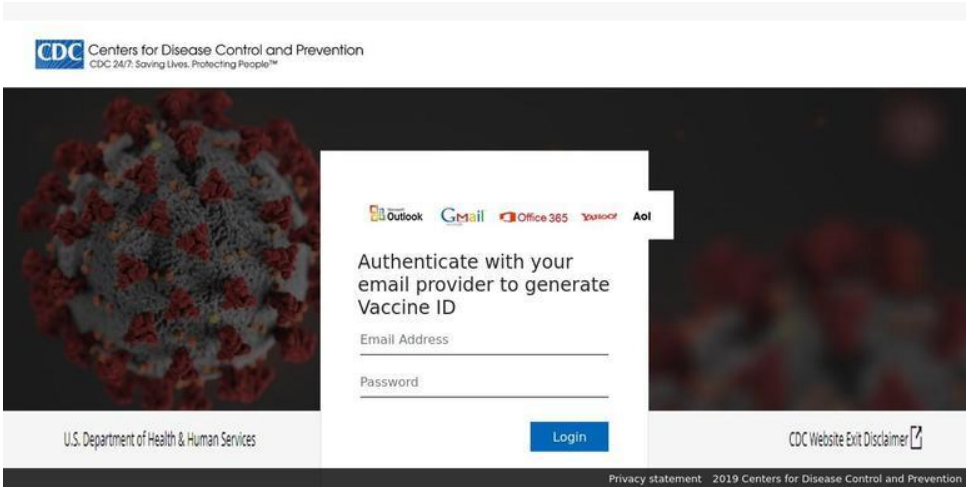
Designing a website from scratch can be time-consuming, especially for cybercriminals busy plotting their next campaign. That's one reason templates are a popular item on the dark web as they offer attackers a ready-built means to fashion their own customized phishing pages.

The spread of the coronavirus has triggered a surge in templates that spoof government agencies and health organizations in an effort to capture personal information from people. In a blog post published Thursday, security provider Proofpoint looks at several virus-themed templates that have been used in phishing attacks.

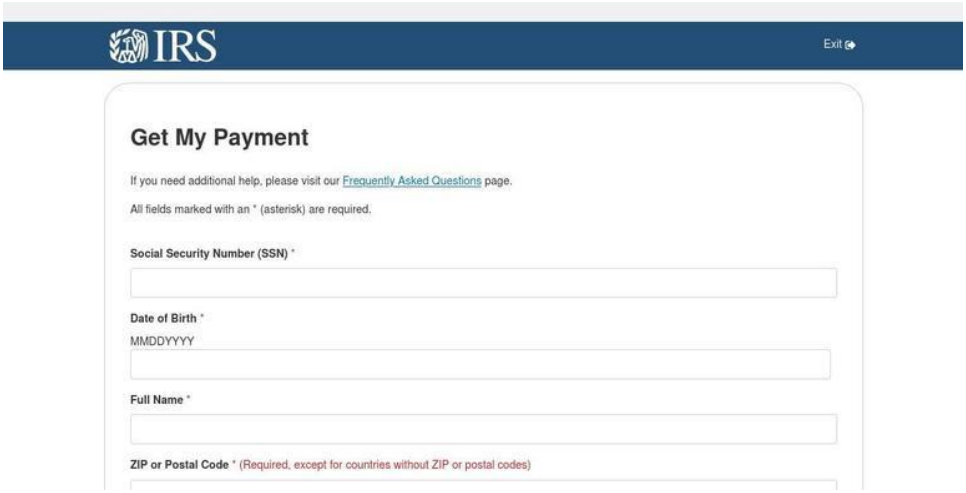
The coronavirus-themed templates found by Proofpoint mimic the brands of such entities as the World Health Organization (WHO), the Internal Revenue Service (IRS), the Centers for Disease Control (CDC), the UK government, the government of Canada, and the government of France. Though most of them are written in English, some are in Japanese, Spanish, Italian, French, Portuguese, and Turkish.
Many of these COVID-19 phishing templates try to entice people by promising information on stimulus payments and financial aid. Looking at the past couple of months, the use of these templates started to grow around the beginning of March, hitting a peak toward the end of the month, and then trailing off over the course of April. The drop-off may reflect the shift toward other types of COVID-19 themes as payments from the IRS and other organizations were already being sent out.

One phishing page template analyzed by Proofpoint copies the look and layout of the WHO's website by adopting the site's logo and color scheme. Designed to be used as part of a credential phishing campaign, the template prompts people to enter a username and password to receive COVID-19 safety information.

Another template geared for credential phishing impersonates the actual site of the US Centers for Disease Control (CDC). The template asks people to "Authenticate with your email provider to generate Vaccine ID." The login window displays logos for Microsoft Outlook, Gmail, Office 365, Yahoo, and AOL, indicating that the attackers are looking for credentials from any of those services.

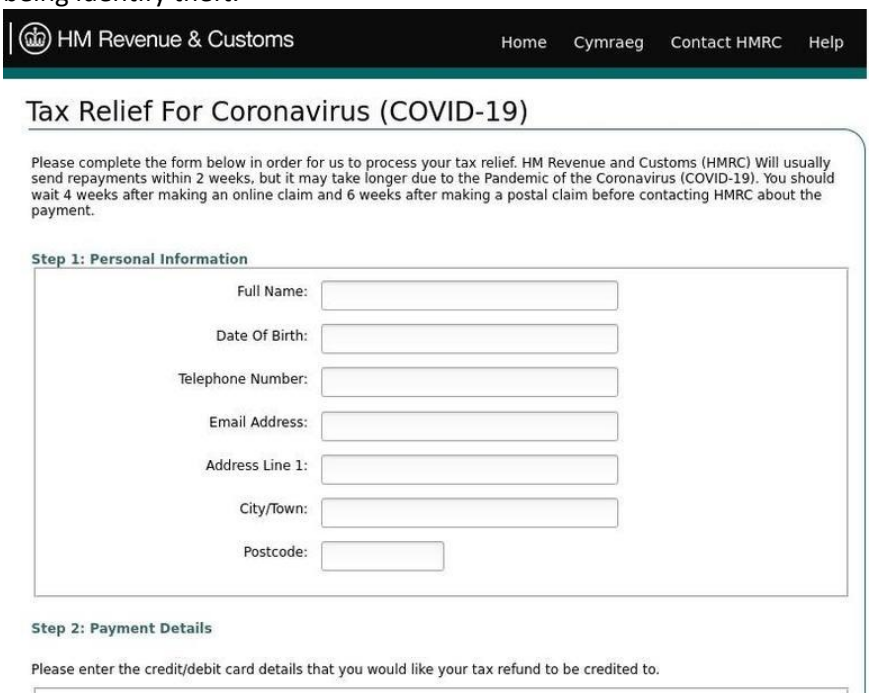


Spoofing the IRS website, a third template promises the visitor a certain amount of money as "financial aid" as part of a COVID-19 relief program. In this instance, one of the pages asks not just for a full name and date of birth but for the person's Social Security number, lending itself to a campaign that could easily be used for identity theft.



Outside the US, one template spoofs the legitimate Canadian Government website and even gives the user a choice of reading the site in English or in French. Promising information on COVID-19 financial support, the template actually is designed to capture names and social insurance numbers. In Canada, a social insurance number is roughly equivalent to a US Social Security number and so is a valuable piece of data for a cybercriminal to obtain.

For use in the United Kingdom, another template impersonates the website of Her Majesty's Revenue and Customs (HMRC), the UK's version of the United States' IRS. Offering to process the visitor's tax relief for the coronavirus, the template asks for a name, date of birth, and full address, with the end goal being identify theft.



Yet another template geared for the UK spoofs the City of Westminster City Council's section of the United Kingdom government website. Promising COVID-19 relief funds, the template is set up to collect all types of personal information, including name, birth date, email address, phone number, address, and mother's maiden name. That maiden name is used as a security question on many websites, thereby giving cybercriminals a useful piece of data for account takeovers.

Finally, a template directed toward people in France mimics the look and feel of the official French government website. This one asks for a name, address, and other personal information in exchange for help on financial assistance from the government over the COVID-19 pandemic.

"Overall, we've seen more than 300 different COVID-19 campaigns (since January 2020) across nearly every industry we track," Proofpoint said in its report. "The threat actors behind these campaigns have run the gamut from well-known, established threat actor groups to unknown individuals. As the COVID-19 situation continues to unfold across the globe, we can expect these kinds of COVID-19 themed attacks to continue, and threat actors to offer additional tools that can make those attacks easier to carry out."